EVALUACIÓN – PRUEBA DE HABILIDADES PRÁCTICAS CCNA

ESNEIDER ALEXANDER URREGO HURTADO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

PROGRAMA DE INGENIERIA EN TELECOMUNICACIONES

CEAD FACATATIVA

2019

EVALUACIÓN – PRUEBA DE HABILIDADES PRACTICAS CCNA

ESNEIDER ALEXANDER URREGO HURTADO

GRUPO 203092_2

DIPLOMADO DE PROFUNDIZACIÓN CISCO

TUTOR

GIOVANNI ALBERTO BRACHO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

PROGRAMA DE INGENIERIA EN TELECOMUNICACIONES

CEAD FACATATIVA

2019

PRUEBA DE HABILIDADES PRACTICAS CCNA

Resumen

Por medio de este trabajo se pretender dar solución a problemas de telecomunicaciones, problemas que se pueden presentar en el ejercicio de nuestra labor profesional, por medio del desarrollo de estos escenarios y en los requerimientos que este trabajo implica, se adquieren habilidades prácticas y de funcionabilidad, que ayudan a tener conocimiento del funcionamiento de las redes de información.

Por medio de las herramientas que ofrece la universidad con la plataforma Cisco y con el programa Packet Tracer, se da solución a las problemáticas propuestas, usando protocolos, configuraciones, enrutamiento, vectores de distancia, tiempo y estado de enlace.

ABSTRACT

Through this work it is intended to solve telecommunication problems, problems that may arise in the exercise of our professional work, through the development of these scenariosand in the requirements that this work implies, practical and functional skills are acquired , which help to have knowledge of the operation of information networks.

Through the tools offered by the university with the Cisco platform and with the Packet Tracer program, the proposed problems are solved, using protocols, configurations, routing, distance vectors, time and link status.

INDICE

Tabla deImágenes

PRUEBA DE HABILIDADES PRACTICAS CCNA

INTRODUCCIÓN

La prueba de habilidades practica que en este trabajo se presenta, tiene como finalidad dar solución a dos escenarios diferentes sobre problemáticas en telecomunicaciones, poniendo a prueba las habilidades de los futuros ingenieros frente a situaciones que se pueden llegar a presentar en el ejercicio de su carrera como pueden ser: iniciación de dispositivos de red, diseñar una red, configurar routers, servidores, switches, suministrar códigos de seguridad, direccionamientos IP, control de acceso, entre otros.

Además debe estar en la capacidad de solucionar problemas y encontrar soluciones a las diversas dificultades que se presentan mientras se construye el código, con las diferentes exigencias que pide la prueba de habilidades práctica, al finalizar los ejercicios, debe estar en la capacidad de redactar un informe detallado de su trabajo, haciendo uso de las herramientas aprendidas durante el Diplomado en Cisco.

.

Objetivos

General

Implementar todos los conocimientos adquiridos durante el Diplomado de Cisco para la resolución de problemas en telecomunicaciones, usando habilidades prácticas y teóricas que se viven desde la experiencia.

Específicos

- Solucionar problemas de telecomunicaciones, usando las herramientas adquiridas en el Diplomado
- Identificar las posibles soluciones e identificar cual es la más viable
- Categorizar los dispositivos a utilizar en el proyecto Pára la solución de una situación
- Crear la configuración de enrutamiento
- Configurar las listas de control de acceso
- Configurar routers, servidores, switches,
- Comprobar la red instalada
- Seguir los parámetros que exige la solución de la guía

1 Escenario 1

Una empresa posee sucursales distribuidas en las ciudades de Bogotá, Medellín y Cali en donde el estudiante será el administrador de la red, el cual deberá configurar e interconectar entre sí cada uno de los dispositivos que forman parte del escenario, acorde con los lineamientos establecidos para el direccionamiento IP, protocolos de enrutamiento y demás aspectos que forman parte de la topología de red

1.1 DESARROLLO:

Se inicia con la configuración básica, se construye la topología, con los requerimientos de la empresa.

1.2 TOPOLOGIA

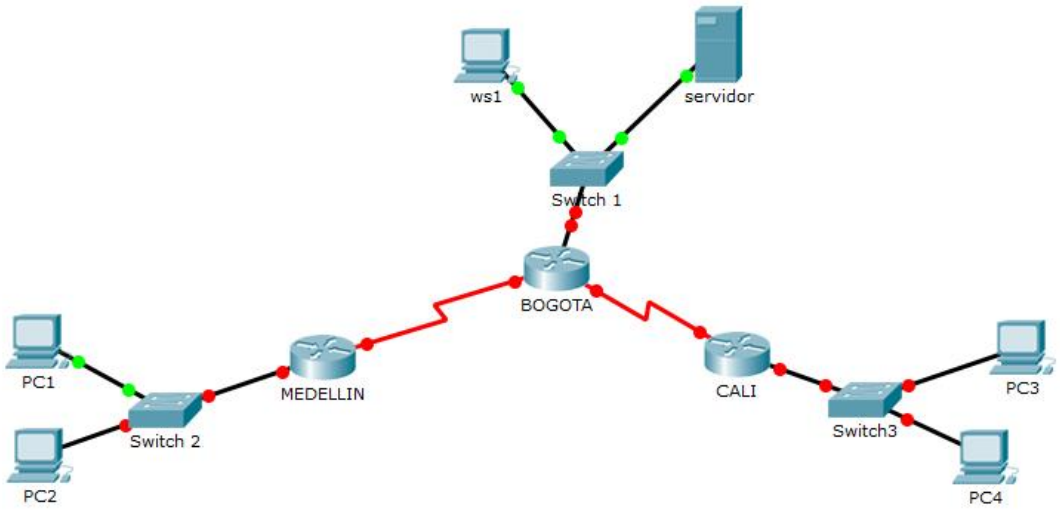


FIGURA 1 TOPOLOGIA

1.3 PARTE 1: ASIGNACIÓN DE DIRECCIONAMIENTO IP.

- ✓ se asigna IP a cada uno de los switch, servidor, PC y routers, tal como se ve en las graficas

1.3.1

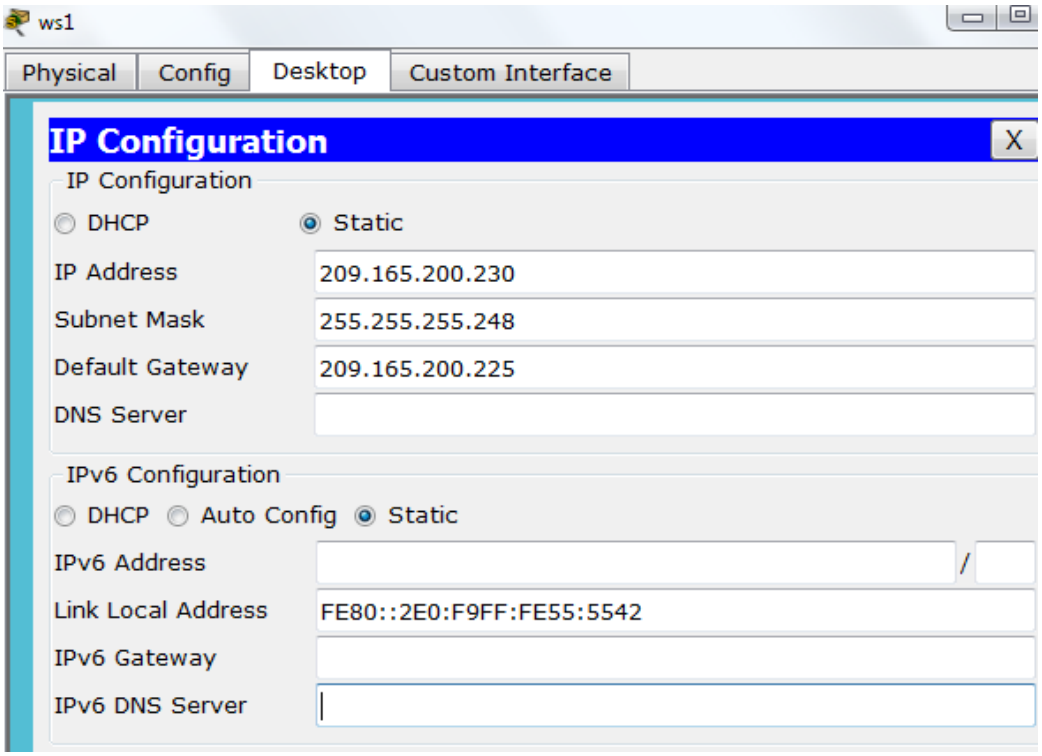


FIGURA2 INTERNET PC

1.3.2

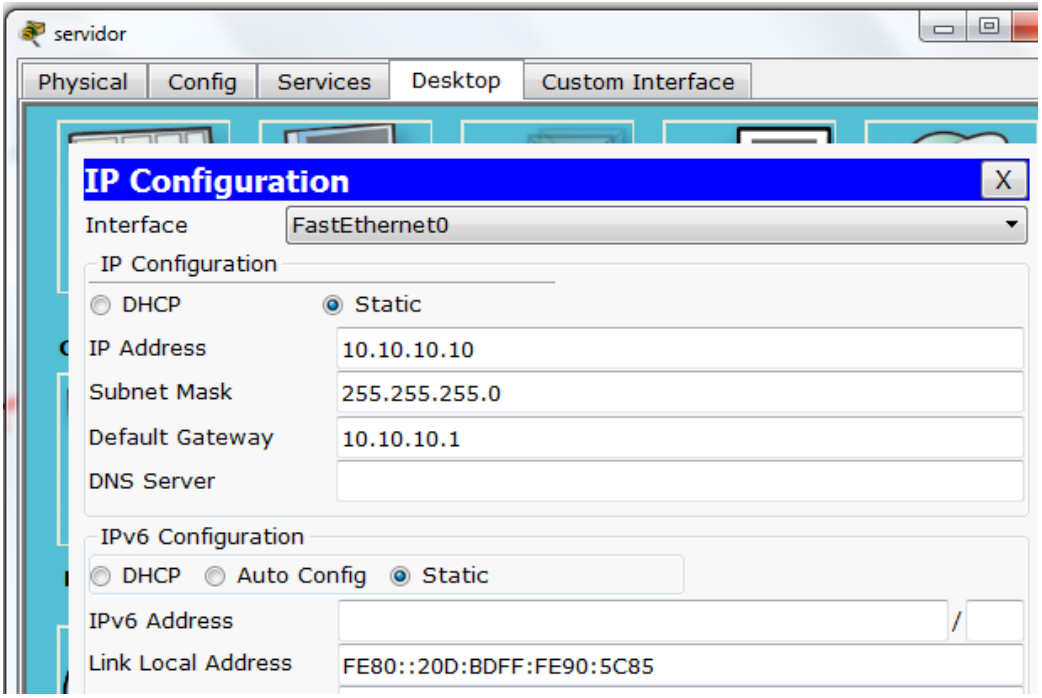


FIGURA 3 WEB SERVER

1.3.3

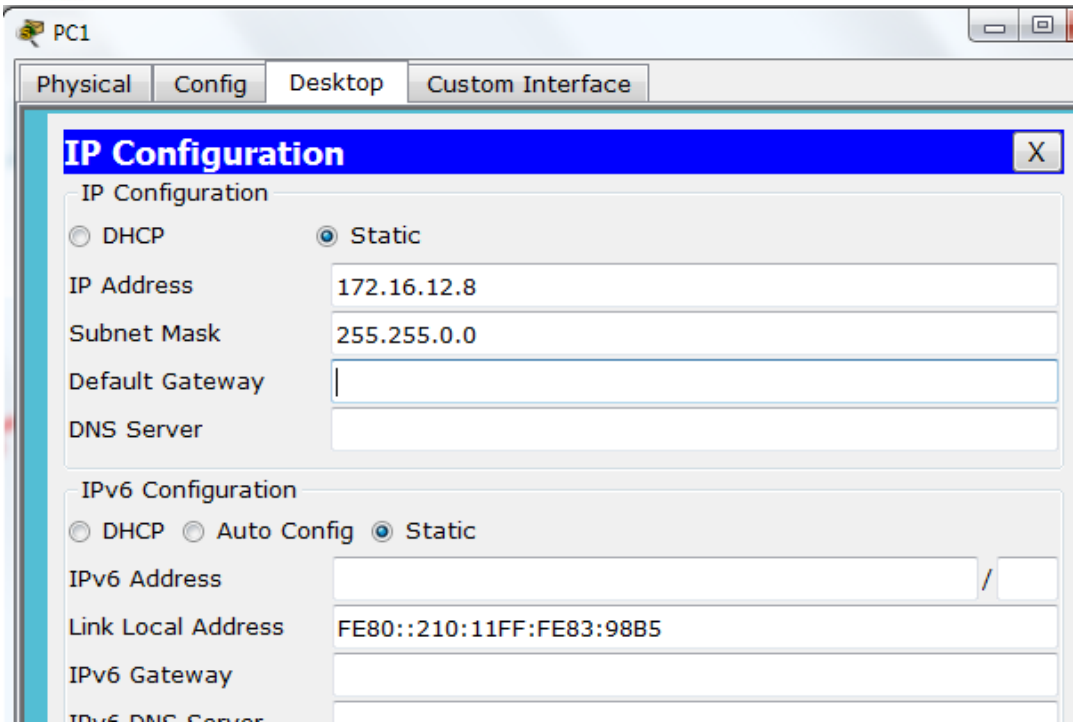


FIGURA 4 PC-1

1.3.4

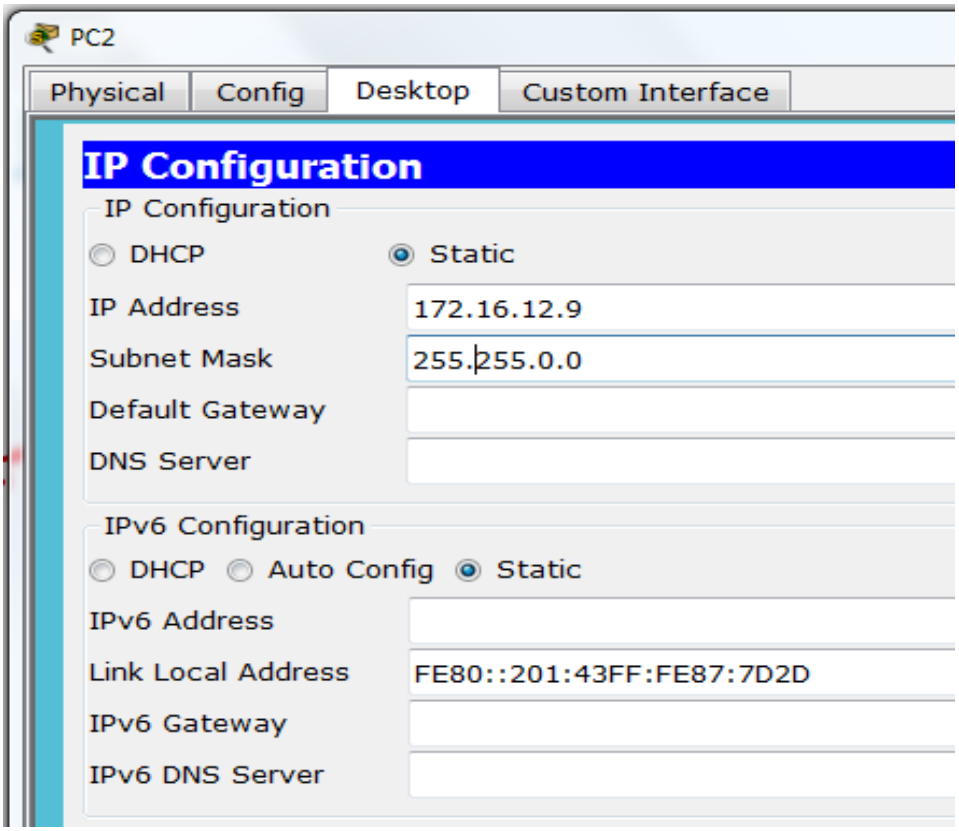


Figura 5 PC-2

1.3.5

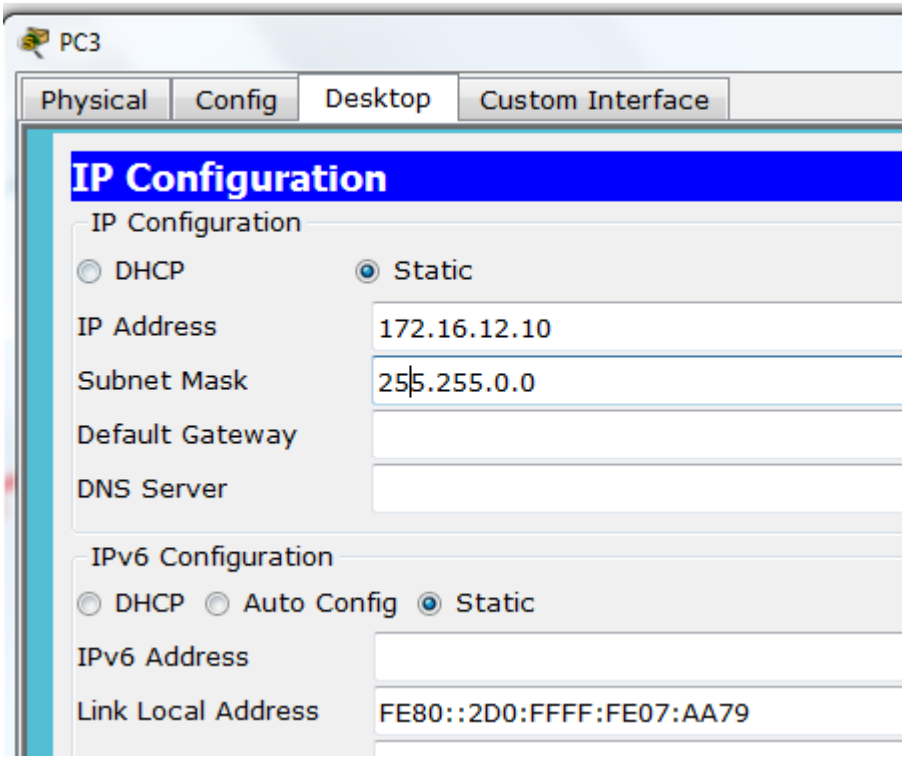


Figura 6 PC-3

1.3.6

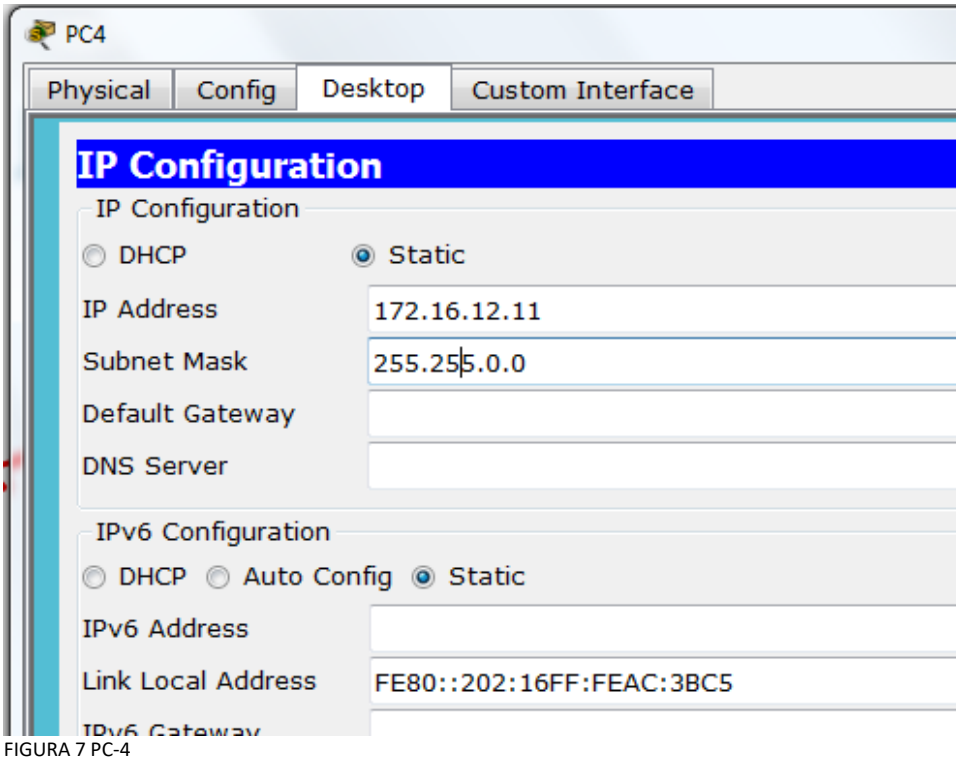


FIGURA 7 PC-4

1.4 PARTE 2: CONFIGURACIÓN BÁSICA.

1.5 Configuración Básica De Dispositivos

Aplicar a cada Router y Switch de la topología, las siguientes configuraciones básicas;

- R1: nombrarlo “Medellín”
- R2: nombrarlo “Bogotá”
- R3: nombrarlo “Cali”
- S1: nombrarlo “Switch1”
- S2: nombrarlo “Switch2
- S3: nombrarlo “Switch3”

✓ Exec Password: class
✓ Console Access Password: cisco
✓ Telnet Access Password: cisco
✓ Encriptar contraseñas
✓ MOTD banner: Prohibido personal no autorizado
✓ A cada Switch deshabilitar DNS lookup

A. TABLA:

	R1	R2	R3
Nombre de Host	**MEDELLIN**	**BOGOTA**	**CALI**
Dirección de Ip en interfaz Serial 0/0	192.268.1.99	192.168.1.98	192.168.1.131
Dirección de Ip en interfaz Serial 0/1	192.168.1.50	192.168.1.130	192.168.1.43
Dirección de Ip en interfaz FA 0/0	192.168.1.33	192.168.1.1	192.168.1.65
Protocolo de enrutamiento	**Eigrp**	**Eigrp**	**Eigrp**
Sistema Autónomo	200	200	200
Afirmaciones de red	192.168.1.0	192.168.1.0	192.168.1.0

FIGURA 8 TABLA DE CONFIGURACION BASICA

a. Después de cargada la configuración en los dispositivos, verificar la tabla de enrutamiento en cada uno de los routers para comprobar las redes y sus rutas.

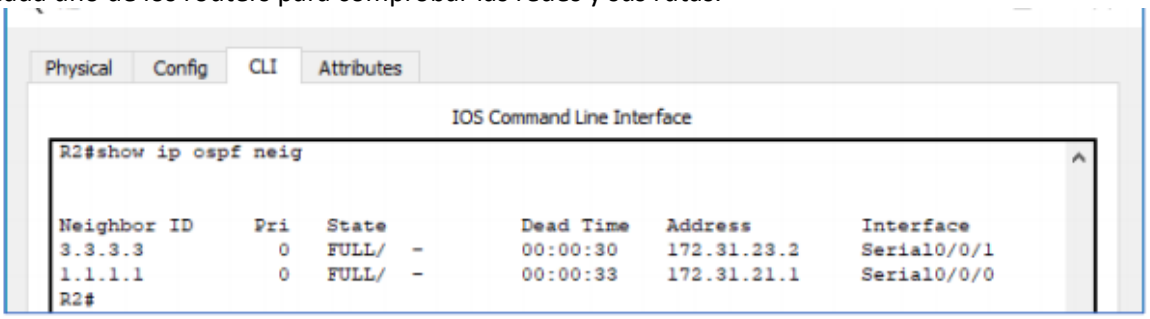


FIGURA 9 VERIFICACION ENRUTAMIENTO

b. Realizar un diagnóstico de vecinos uando el comando cdp.

1.6 D DIAGNOSTICO DE VECINOS COMANDO CDP:

c. switch2#show cdp ne
d. switch2#show cdp neighbors

e. **capability codes: R - Rouer, T - Trans Bridge, B - Sourse route bridge**
f. **s - switch,H - host, I - ICMP, r - repeater, P - Phone**
g. **Device ID Local intrfce holdtne capability platforn port ID**
h. **switch1 fas 0/1 12 2950 Fas 0/2**
i. **switch2#show cdp neighbors det**
j. **switch2#show cdp neighbors detail**
k.
l. **Device ID: Switch1**
m. **entry address : 10.10.1.1**
n. **platfora: cisco 2950, capabilities: switch**
o. **interface: fastIthernet0/1, port ID (outgoin port): fastIthernet0/2**
p. **holdtime: 121**
q.
r. **version:**
s. **cisco internetwork operating systen sofware**
t. **IOS (tn) c2950 software (c2950-I6Q4L2-M), version 12.1(22)ea4, release software(fcl)**
u. **advertisenent version:2**
v. **duplex: full**
w. E. realizar prueba de conectividad usando comando ping
x. **PC>ping 10.10.1.1**
y.
z. **pinging 10.10.1.1 with 32 bytes of data:**
aa.
bb. **replY from 10.10.1.1: bytes=32 time=3lms TTL=255**
cc. **replY from 10.10.1.1: bytes=32 time=3lms TTL=255**
dd. **replY from 10.10.1.1: bytes=32 time=3lms TTL=255**
ee. **replY from 10.10.1.1: bytes=32 time=3lms TTL=255**
ff.
gg. **Ping statistics for 10.10.1.1:**
hh. **packets: sent = 4, received = 4, lost = 0 (04 loss),**
ii. **approximate round trip times in milli-seconds:**
jj. **mininum = 15ms, maxinun = 31ms, average = 27ms**

c. Realizar una prueba de conectividad en cada tramo de la ruta usando Ping.

1.7 PRUEBA DE CONECTIVIDAD CON PING

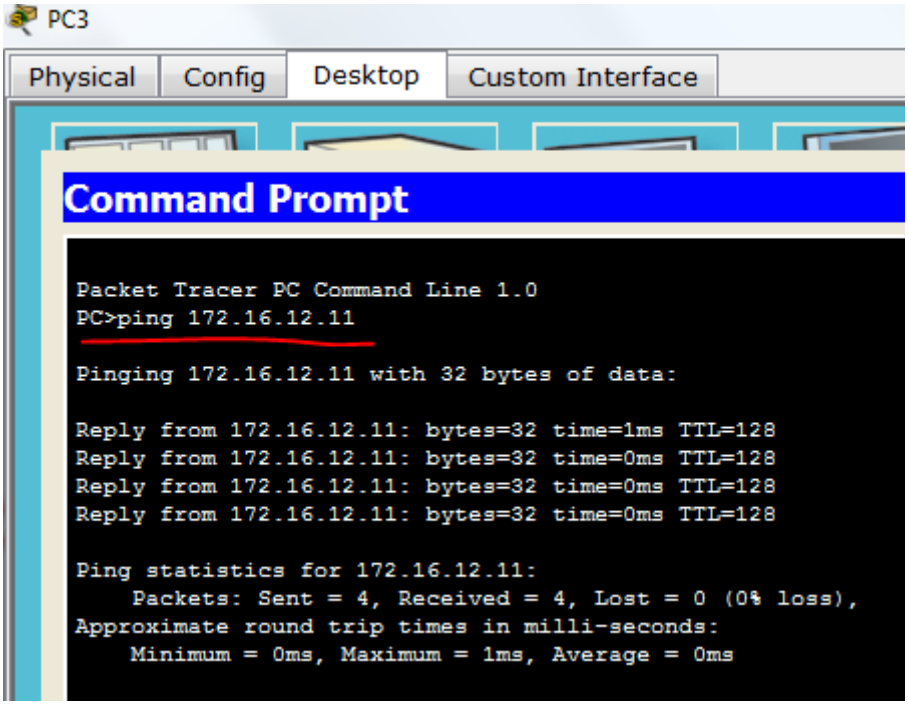


Figura 10 pin PC 3 -medellin

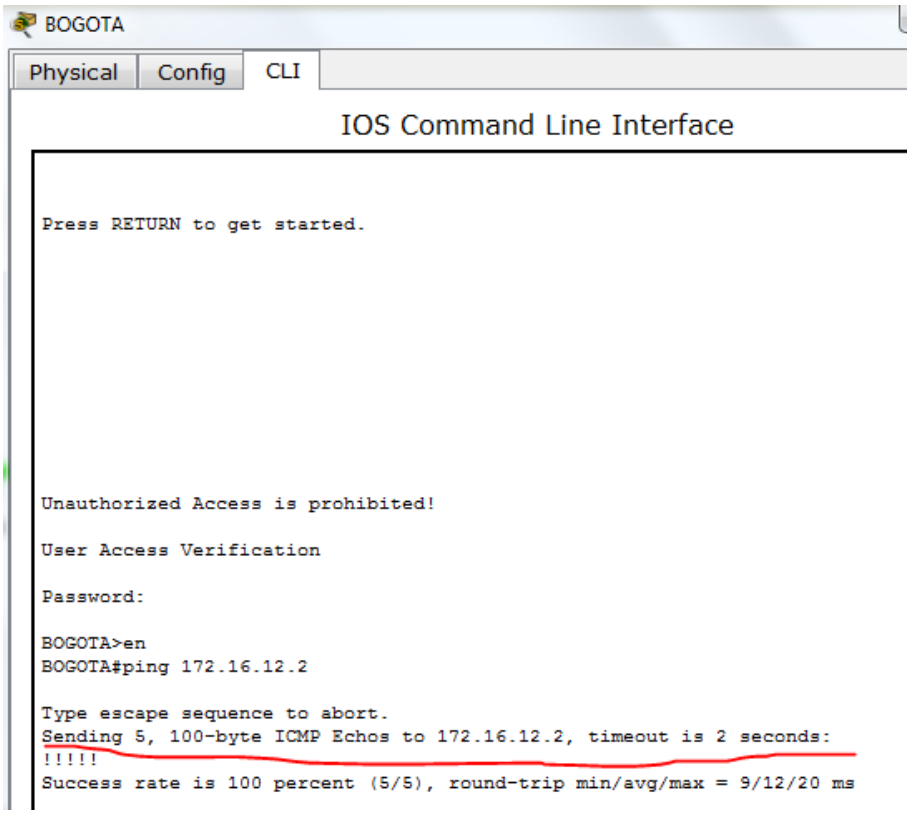


FIGURA 11 PING BOGOTA- MEDELLIN

Se hace ping Bogota a servidor

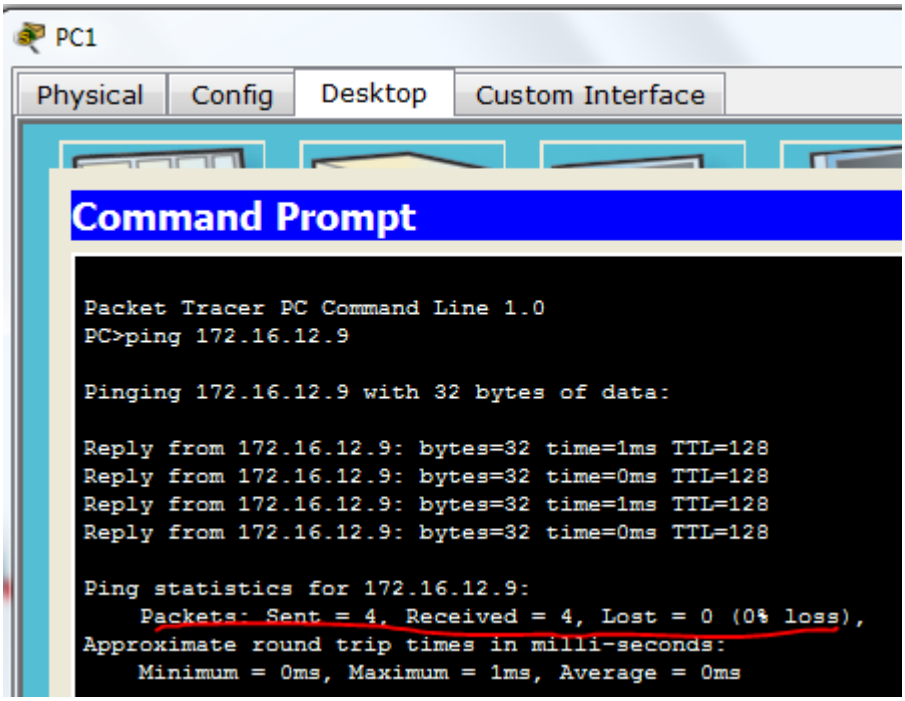


figura 12 ping Bogot- SERVIDOR

PARTE 3

.1.8 CONFIGURACIÓN DE DISPOSITIVOS DE ENRUTAMIENTO:

En las siguientes gráficas, se puede observar las configuraciones que se le dieron a cada uno de los routers, y el código.

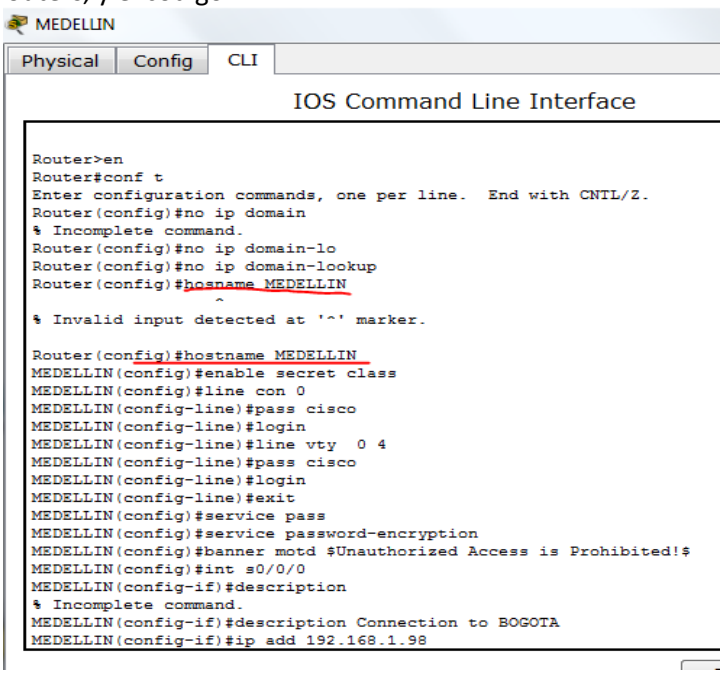


FIGURA 13 DISPOSITIVO DE ENRUTAMIENTO MEDELLIN

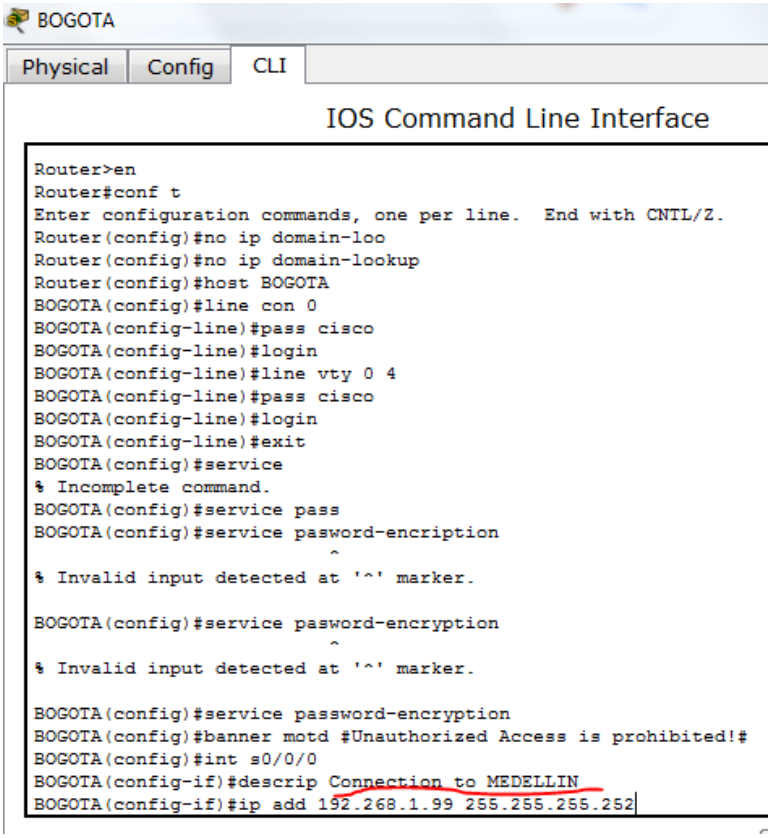


FIGURA 14 DISPOSITIVO DE ENRUTAMIENTO BOGOTA

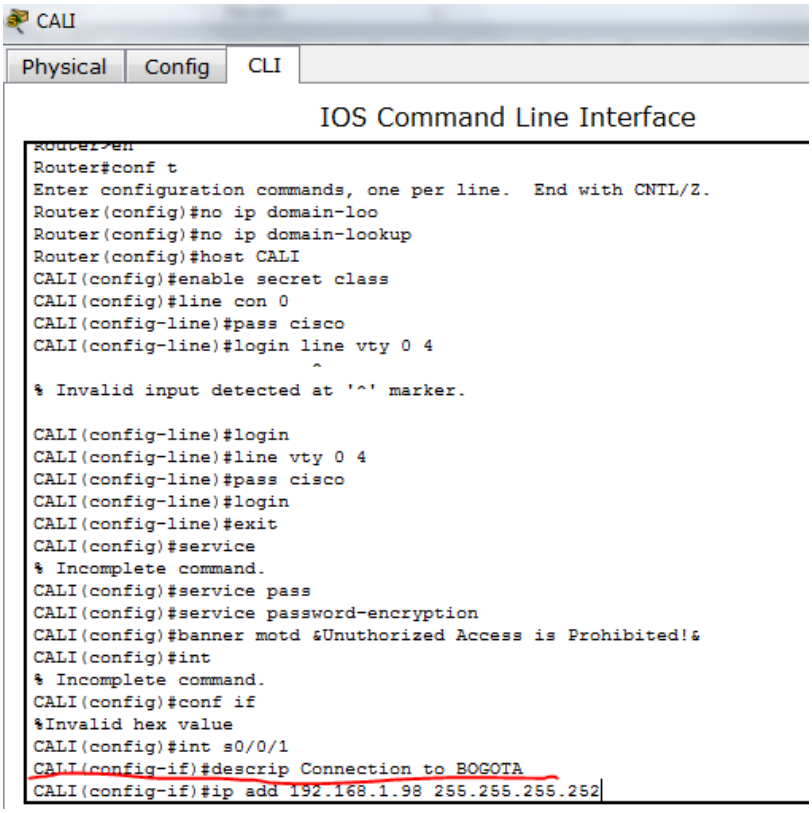


FIGURA 15 DISPOSITIVO DE ENRUTAMIENTO CALI

1.9 Asignar el protocolo de enrutamiento EIGRP a los routers considerando el direccionamiento diseñado.

Se Habilita el proceso de routing EIGRP en cada router con el número de AS 1. Se muestra la configuración para el **R1**. (Medellín)

Medellín(config)# router eigrp 1

Observaciones: en la actualidad, Packet Tracer no permite la configuración de una ID de router EIGRP

a. Verificar si existe vecindad con los routers configurados con EIGRP.

En cada router, se configura EIGRP para comunicar las subredes específicas enlazadas directamente. Como ejemplo tenemos la configuración para el **R1**.(Medellín)

```
Medellin(config-router)#network 172.16.1.0.0.0.0.255
Medellin(config-router)#network 172.16.3.0.0.0.0.3
Medellin(config-router)#network 192.168.10.4.0.0.0.3
```

Los tres routers deberán tener dos vecinos en la lista. El resultado para el **R1 (Medellín)** debe ser equivalente a lo siguiente:

```
IP-EIGRP neighbors for process 1


H    Address       interface   hold uptime    SRTT    rto       Q          SEG0
O   172.16.3.2      Se0/0/0      14 00:25:05    40    1000       0          28
1  192.168.10.6     Se0/0/1      12  00:13:29   40     1000      0          31
```

b. Realizar la comprobación de las tablas de enrutamiento en cada uno de los routers para verificar cada una de las rutas establecidas.

1.9 PARTE 3. PROTOCOLO DE ENRUTAMIENTO

Configuration	Specification
Router ID R1	**1.1.1.1**
Router ID R2	**2.2.2.2**
Router ID R3	**3.3.3.3**
Configurar todas las interfaces LAN como pasivas	
Establecer el ancho de banda para enlaces seriales en:	**128 Kb/s**
Ajustar el costo en la métrica de S0/0 a:	**7500**

FIGURA 16 PROTOCOLO ENRUTAMIENTO

Dispositivo	destino	Dirección IP	Mascara de sub red	Gateway predeterminado
Router 1	Medellín	192.268.199	255.255.255.252	2001:DB8:ACAD:12::1/64
Router 2	Bogotá	192.168.1.98	255.255.255.252	2001:DB8:ACAD:12::2/64
Router 3	Cali	192.168.1.131	255.255.255.252	2001:DB8:ACAD:12::3/64

FIGURA 17 COMPROBACION DE ENRUTAMIENTO

c. Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

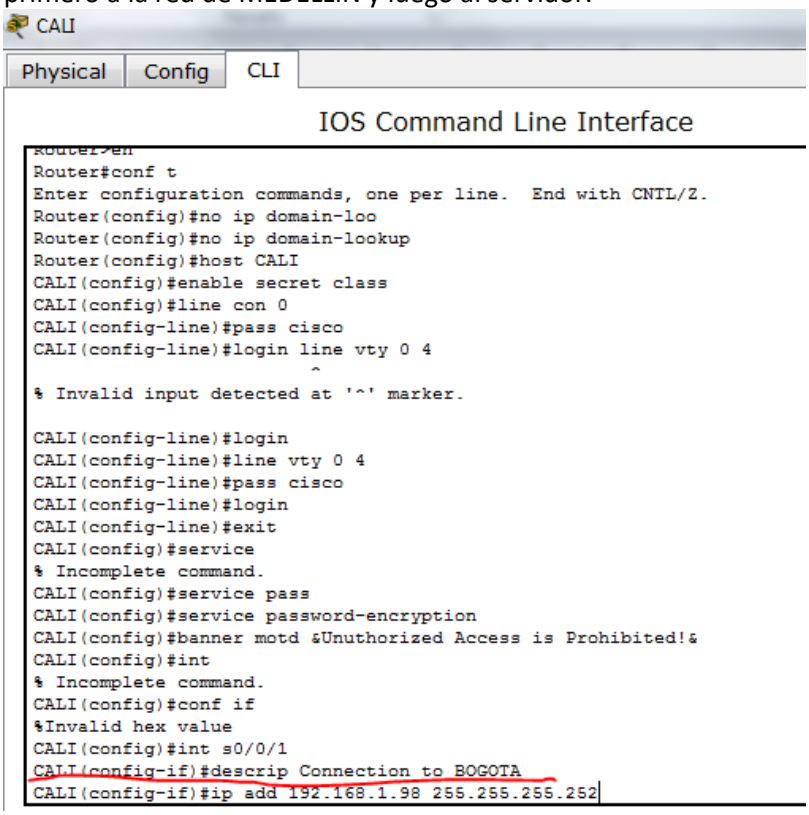


FIGURA 18 configuración de dispositivos de enrutamiento R1

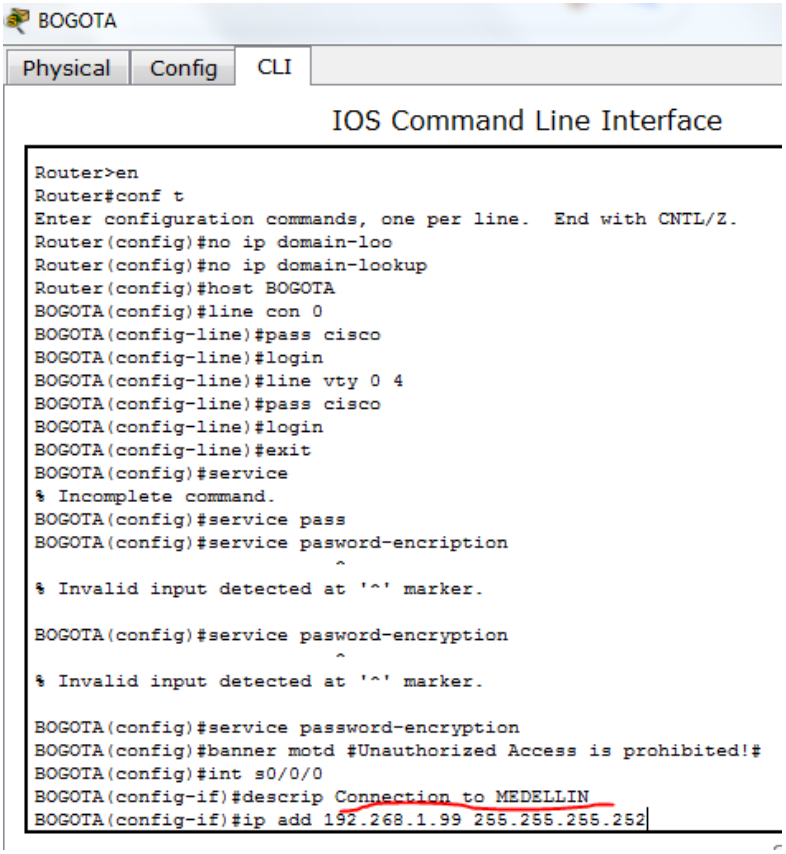


FIGURA 18 configuración de dispositivos de enrutamiento R2

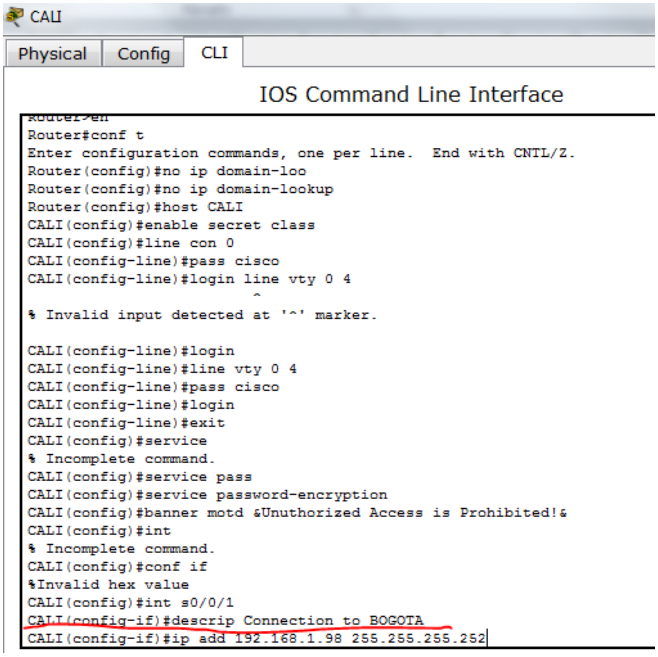


FIGURA 19 configuración de dispositivos de enrutamiento R3

1.10 Realizar un diagnóstico para comprobar que cada uno de los puntos de la red se puedan ver y tengan conectividad entre sí. Realizar esta prueba desde un host de la red LAN del router CALI, primero a la red de MEDELLIN y luego al servidor.

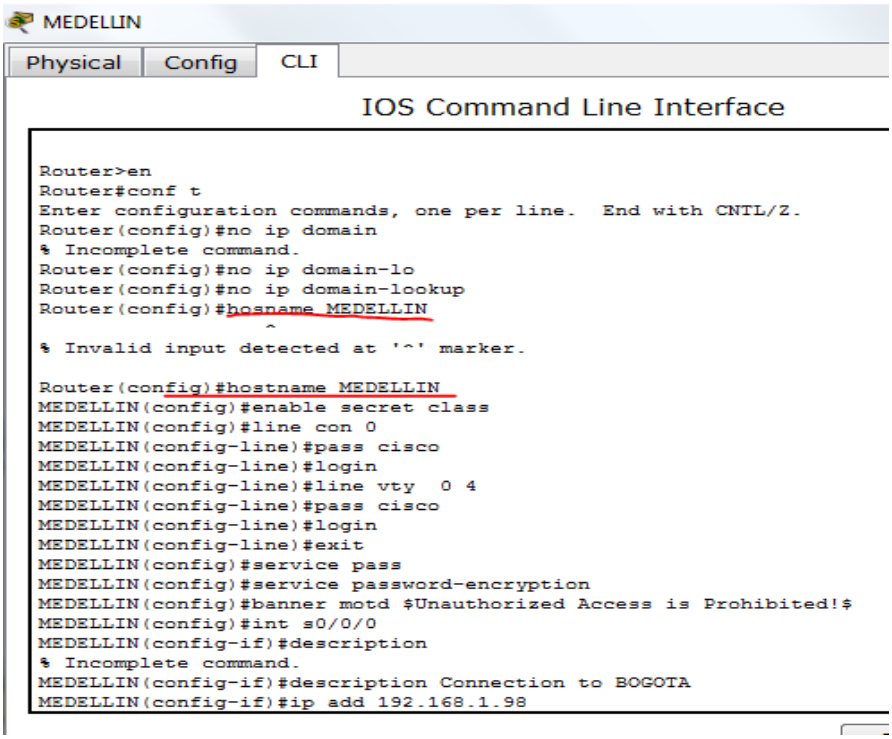


FIGURA 20 PUNTOS DE CONECTIVIDAD

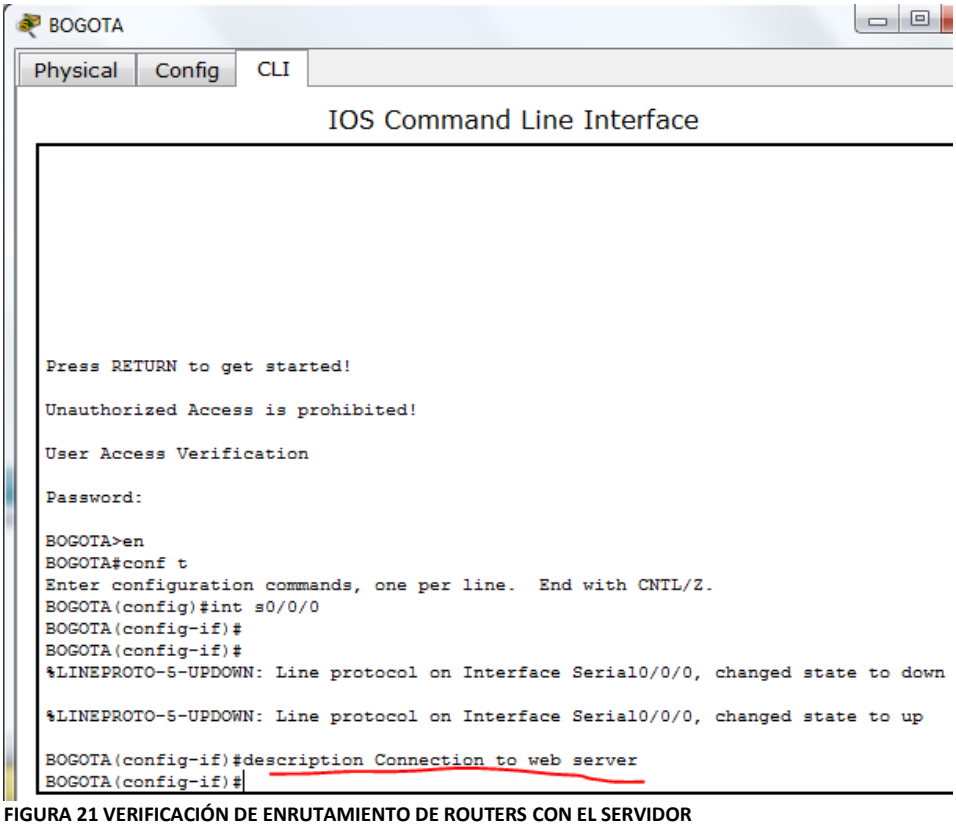


FIGURA 21 VERIFICACIÓN DE ENRUTAMIENTO DE ROUTERS CON EL SERVIDOR

PARTE 4

1.11 CONFIGURACION DE LAS LISTAS DE CONTROL DE ACCESO

En este momento cualquier usuario de la red tiene acceso a todos sus dispositivos y estaciones de trabajo. El jefe de redes le solicita implementar seguridad en la red. Para esta labor se decide configurar listas de control de acceso (ACL) a los routers.

Las condiciones para crear las ACL son las siguientes:
a. Cada router debe estar habilitado para establecer conexiones Telnet con los demás routers y tener acceso a cualquier dispositivo en la red.

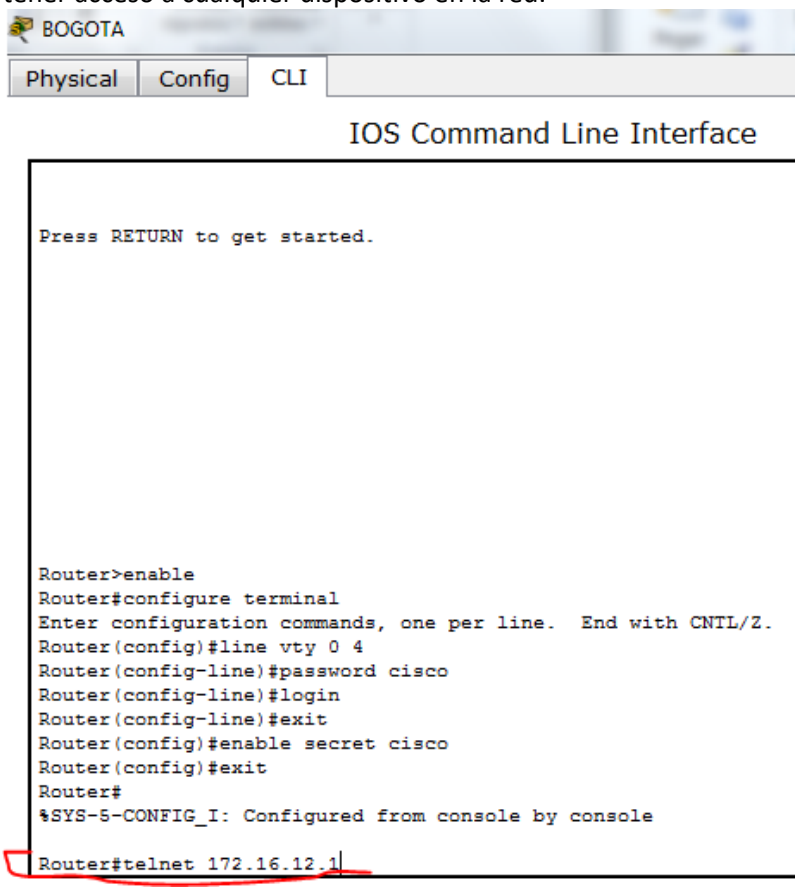


FIGURA 21 CONFIGURACION TELNET

b. El equipo WS1 y el servidor se encuentran en la subred de administración. Solo el servidor de la subred de administración debe tener acceso a cualquier otro dispositivo en cualquier parte de la red.
c. Las estaciones de trabajo en las LAN de MEDELLIN y CALI no deben tener acceso a ningún dispositivo fuera de su subred, excepto para interconectar con el servidor:

A continuación, se realizará unos pasos de ACL extendida en R2 para proteger la red del tráfico que genera el acceso a internet.

Se configura las listas de control de acceso ACL a los routers con el siguiente código controlar el acceso:

R2#conf t

```
CALI(config)#access-list 100 permit tcp any host 209.165.200.229 eq www
CALI(config)#access-list 100 permit icmp any any echo-reply
CALI(config)#int f0/0
(config-if)#ip access-group 100 in
R2(config-if)#exit
```

Habilitamos el router para establecer conexión TELNET y tener acceso a cualquier conexión de la red

```
MEDELLIN1(config)#Ip nat inside source list HOST interface s0/0 overload
MEDELLIN1(config)#int s0/0
MEDELLIN1(config-if)#ip nat outside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/1
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/2
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#int s0/3
MEDELLIN1(config-if)#ip nat inside
MEDELLIN1(config-if)#exit
MEDELLIN1(config)#exit
MEDELLIN1#show ip nat
translation
```

```
CALI>en
CALI #conf t
CALI (config)#ip access-list standard HOST
CALI (config-std-nacl)#permit 172.29.0.0 0.0.0.255 CALI
(config)#Ip nat inside source list HOST interface s0/0
overload
CALI(config)#int s0/0
CALI(config-if)#ip nat outside
CALI(config-if)#exit
CALI|(config)#int s0/1
CALI(config-if)#ip nat inside
 CALI(config-if)#exit
BOGOTA1(config)#int s0/2 SERVIDOR
SERVIDOR(config-if)#ip nat inside
SERVIDOR (config-if)#exit
SERVIDOR (config)#int s0/3
SERVIDOR (config-if)#ip nat inside
```

SERVIDOR (config-if)#exit
SERVIDOR (config)#exit
SERVIDOR #show ip nat translation

1.12 Parte 5: Comprobación de la red instalada.

a. Se debe probar que la configuración de las listas de acceso fue exitosa.
FIGURA

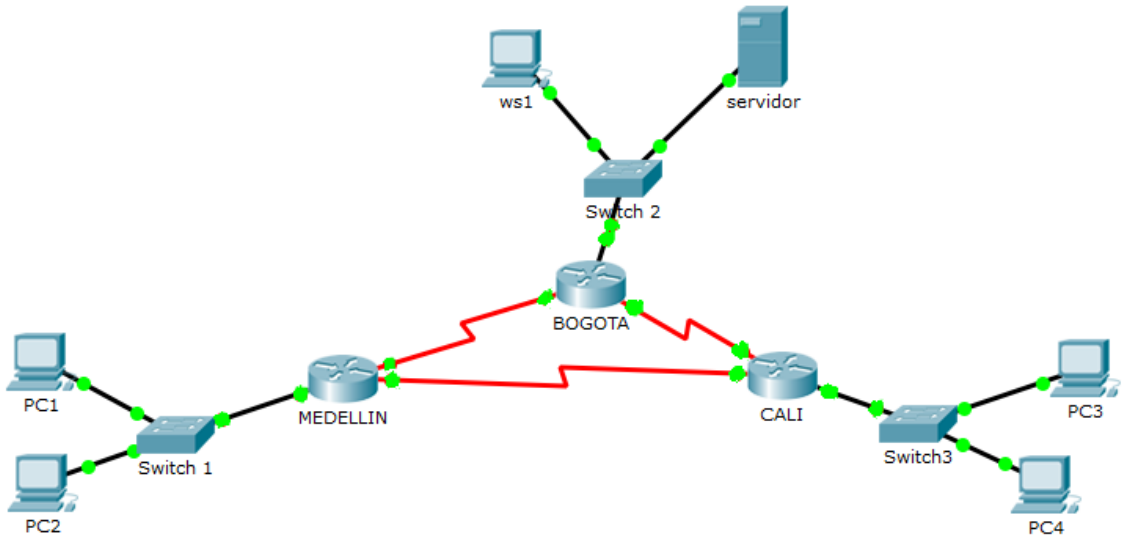


FIGURA23 CONEXIÓN EXITOSA

```
Bogota#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
Bogota(config)#ip access-list standard ADMIN
Bogota(config-std-nacl)#permit host 172.31.21.1
Bogota(config-std-nacl)#exit
Bogota(config)#line vty 0 4
Bogota(config-line)#access-class ADMIN in
Bogota(config-line)#
```

Comprobar y Completar la siguiente tabla de condiciones de prueba para confirmar el óptimo funcionamiento de la red

	ORIGEN	DESTINO	RESULTADO
TELNET	Router MEDELLIN	Router CALI	ok
	WS_1	Router BOGOTA	ok
	Servidor	Router CALI	ok
	Servidor	Router MEDELLIN	ok

TELNET	LAN del Router MEDELLIN	Router CALI	ok
	LAN del Router CALI	Router CALI	ok
	LAN del Router MEDELLIN	Router MEDELLIN	ok
	LAN del Router CALI	Router MEDELLIN	ok
PING	LAN del Router CALI	WS_1	ok
	LAN del Router MEDELLIN	WS_1	ok
	LAN del Router MEDELLIN	LAN del Router CALI	ok
PING	LAN del Router CALI	Servidor	ok
	LAN del Router MEDELLIN	Servidor	ok
	Servidor	LAN del Router MEDELLIN	ok
	Servidor	LAN del Router CALI	Ok
	Router CALI	LAN del Router MEDELLIN	Ok
	Router MEDELLIN	LAN del Router CALI	ok

FIGURA 22 COMPROBACION DE LA RED

2 ESCENARIO 2.

Una empresa tiene la conexión a internet en una red Ethernet, lo cual deben adaptarlo para facilitar que sus routers y las redes que incluyen puedan, por esa vía, conectarse a internet, pero empleando las direcciones de la red LAN original.

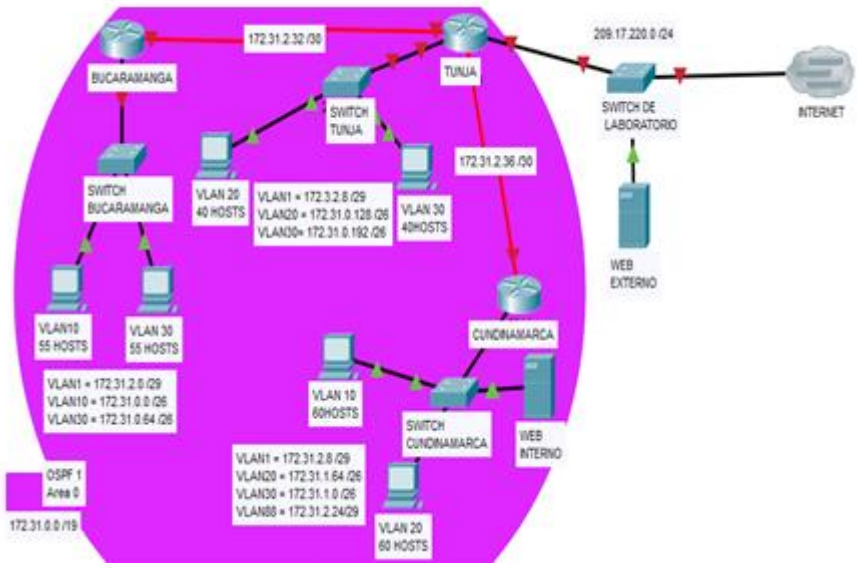


FIGURA 24 CONEXIÓN ESCENARIO 2 INTERNET EN UNA ETHERNET

2.1 Desarrollo

Los siguientes son los requerimientos necesarios:

1. Todos los routers deberán tener los siguiente:
   - Configuración básica.

2.2 TOPOLOGIA

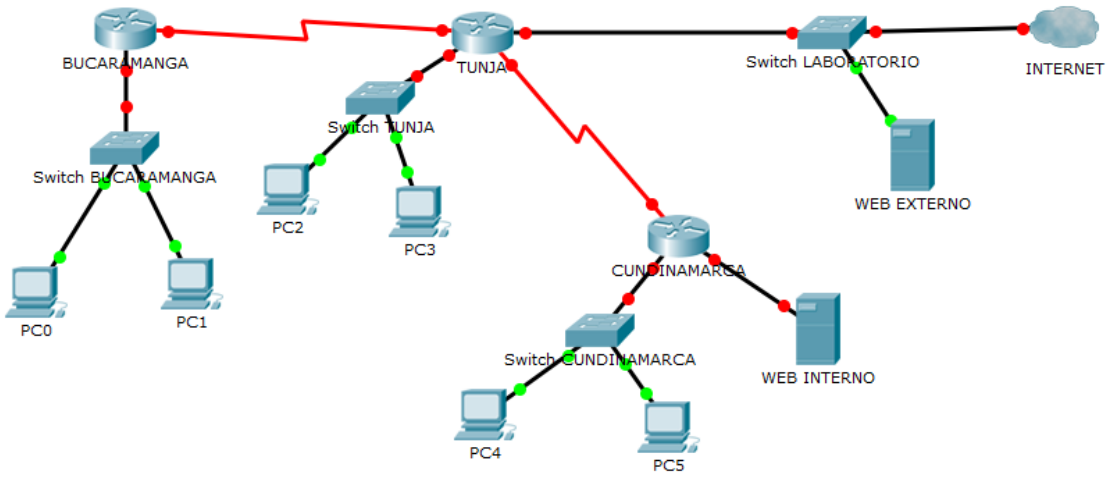


FIGURA 25 TOPOLOGIA

2.3 Cifrado de contraseñas.

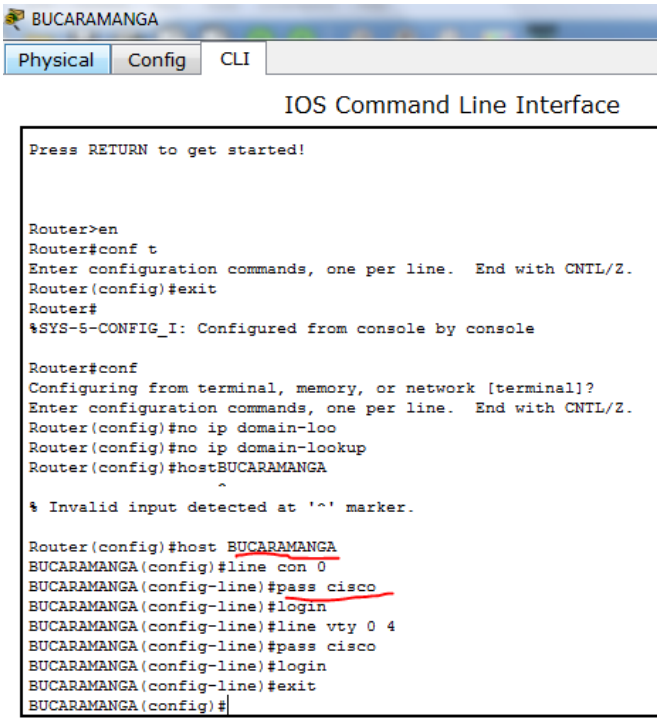


FIGURA 26 CONFIGURACION BASICA

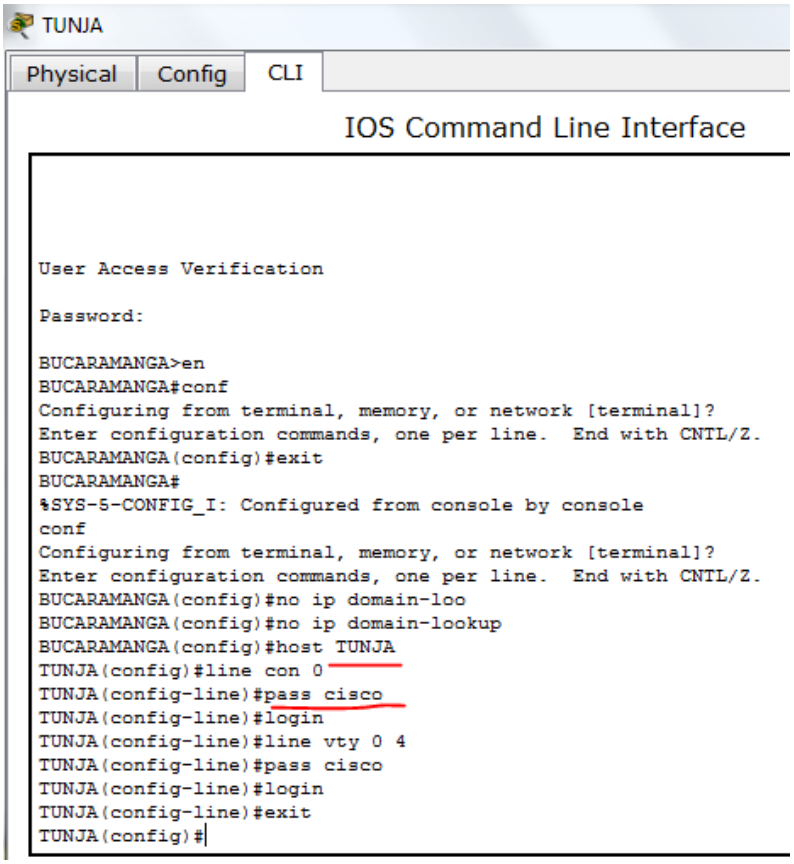


FIGURA 27 CONFIGURACION BASICA TUNJA

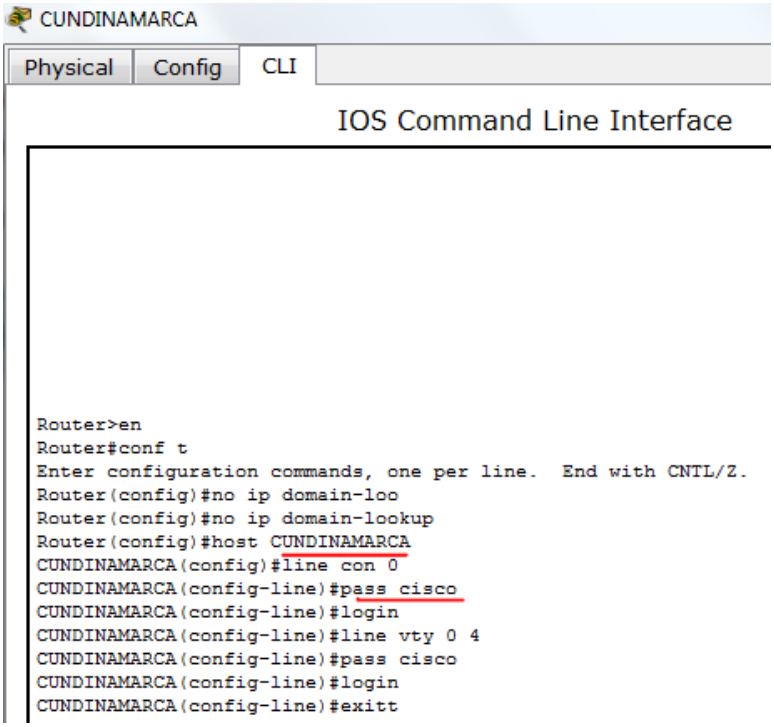
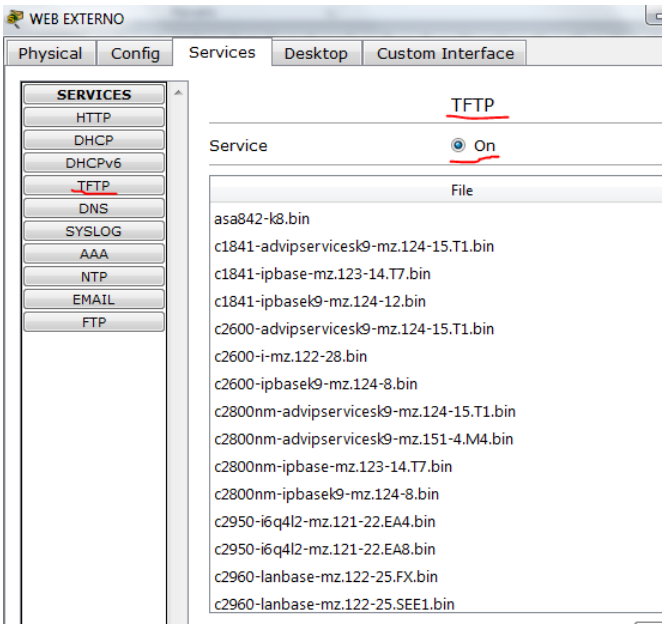


FIGURA 28 CONFIGURACION CUNDINAMARCA

2.4 Establezca un servidor TFTP y almacene todos los archivos necesarios de los routers.



2.5 El DHCP deberá proporcionar solo direcciones a los hosts de Bucaramanga y Cundinamarca

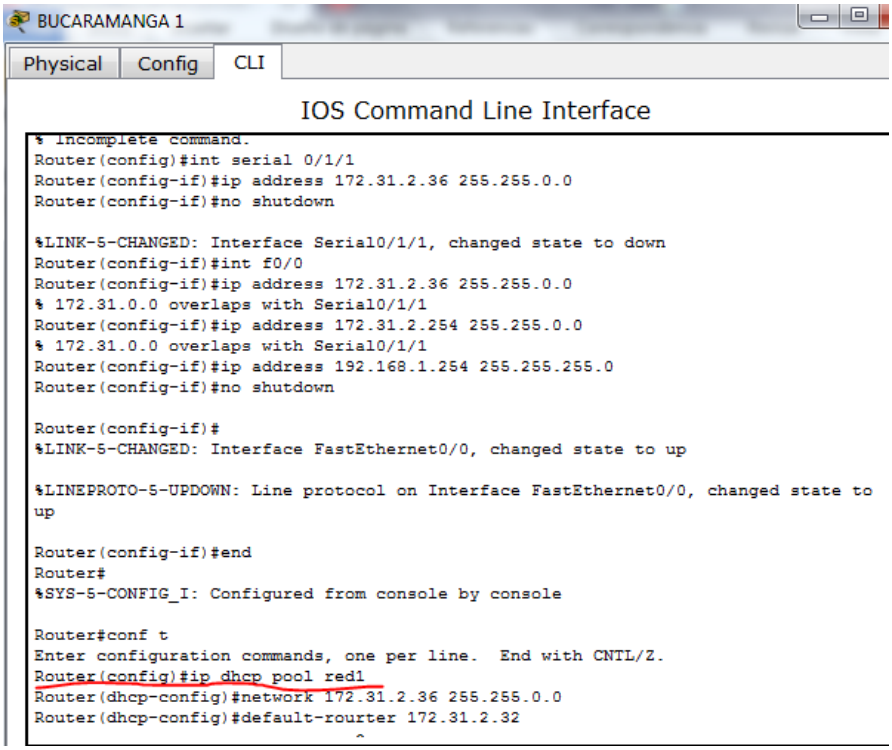


FIGURA 29 DHCP

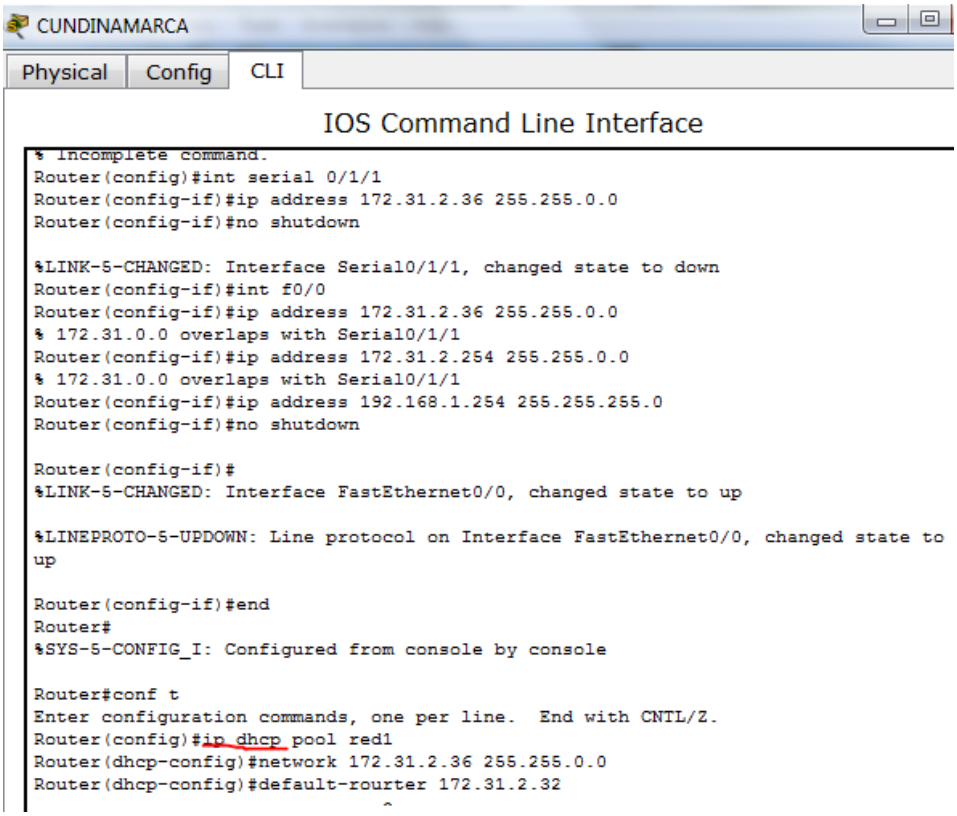


FIGURA 30 DHCP CUNDINAMARCA

2.6 El web server deberá tener NAT estático y el resto de los equipos de la topología emplearan NAT de sobrecarga (PAT).

```
ip nat inside source static 1.1.1.1 2.2.2.2 route-map R1 reversible
!
ip access-list extended ACL-A
permit ip any 30.1.10.128 0.0.0.127'
route-map R1 permit 10
match ip address ACL-A
```

Aspectos a tener en cuenta

- Habilitar VLAN en cada switch y permitir su enrutamiento.
- Enrutamiento OSPF con autenticación en cada router.

Bucaramanga

```
interface Loopback0
  ip address 70.70.70.70 255.255.255.255
 !
 interface Serial0
```

```
  ip address 192.16.64.2 255.255.255.0
  ip ospf message-digest-key 1 md5 c1$c0

!--- Message digest key with ID "1" and !--- Key value (password) is set
as "c1$c0 ".

  clockrate 64000
 !
 router ospf 10
  network 192.16.64.0 0.0.0.255 area 0
  network 70.0.0.0 0.255.255.255 area 0
 area 0 authentication message-digest -->

!--- MD5 authentication is enabled for !--- all interfaces in Area 0.
```

Tunja

```
interface Loopback0
 ip address 172.16.10.36 255.255.255.240
!
interface Serial0
 ip address 192.16.64.1 255.255.255.0
 ip ospf message-digest-key 1 md5 c1$c0

!--- Message digest key with ID "1" and !--- Key (password) value is set
as "c1$c0 ".

!
router ospf 10
 network 172.16.0.0 0.0.255.255 area 0
 network 192.16.64.0 0.0.0.255 area 0
 area 0 authentication message-digest

!--- MD5 authentication is enabled for !--- all interfaces in Area 0.
```

Cundinamarca

```
  show ip ospf interface serial0
  Serial0 is up, line protocol is up
  Internet Address 192.16.64.1/24, Area 0
  Process ID 10, Router ID 172.16.10.36, Network Type POINT_TO_POINT,
. Cost: 64
  Transmit Delay is 1 sec, State POINT_TO_POINT,
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
  Hello due in 00:00:04
  Index 2/2, flood queue length 0
  Next 0x0(0)/0x0(0)
  Last flood scan length is 1, maximum is 1
  Last flood scan time is 0 msec, maximum is 4 msec
  Neighbor Count is 0, Adjacent neighbor count is 0
  Suppress hello for 0 neighbor(s)
  Simple password authentication enabled
```

2.7 Servicio DHCP en el router Tunja, mediante el helper address, para los routers Bucaramanga y Cundinamarca.

Accedemos privilegiado, luego configuración terminal

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Colocamos un nombre al router en este caso Bucaramanga

```
Router(config)#hostname Bucaramanga
```

Creamos el rango de ip quitadas del conjunto pool de direcciones que podrá . . asignar el servicio indicando la ip inicial y final del rango.

```
Bucaramanga (config)#ip dhcp excluded-addres 172.31.2.32  172.31.2.36
```

-

Ponemos un nombre al rango del servidor DHCP

```
Bucaramanga(config)#ip dhcp pool DHCP_LAN_VENTAS
```

Definimos la red a la que dara servicio de DHCP

```
Bucaramanga(dhcp-config)#network 172.31.2.33 255.255.255.0
```

Puerta de enlace que ofrece al DHCP

```
Bucaramanga (dhcp-config)#default-router 172.31.2.34
```

Para terminar el DNS que entregará al DHCP

```
Bucaramanga(dhcp-config)#dns-server 8.8.8.8
```

Se debe tener en cuenta copiar la configuración del router que en este momento estan ejecutándose, en la configuración de inicio del router, en caso de que haya un bajón de energía o reinicio perderíamos la mayoría de información esto se hace con el siguiente comando:

```
Bucaramanga>enable
Bucaramanga#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

2.8 Configuración de NAT estático y de sobrecarga.

```
Tunja# show ip nat translations
Pro Inside global Inside local Outside local Outside global
tcp 209.165.200.226:51839 192.168.10.10:51839 209.165.201.1:80
209.165.201.1:80
tcp 209.165.200.226:42558 192.168.11.10:42558 209.165.202.129:80
209.165.202.129:80
Tunja#
```

Utilizamos el comando nat statistics comprueba las nat que haya asignado una dirección para ambas traducciones

```
Tunja# clear ip nat statistics
Tunja# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Peak translations: 2, occurred 00:00:05 ago
Outside interfaces:
 Serial0/0/1
Inside interfaces:
 Serial0/1/0
Hits: 4 Misses: 0
CEF Translated packets: 4, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 3] access-list 1 pool NAT-POOL2 refcount 2
pool NAT-POOL2: netmask 255.255.255.224
 start 209.165.200.226 end 209.165.200.240
 type generic, total addresses 15, allocated 1 (6%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
Tunja#
```

Listas de control de acceso:

2.9 Los hosts de VLAN 20 en Cundinamarca no acceden a internet, solo a la red interna de Tunja.

```
CUNDINAMARCA(confit)#access-list   1   deny   172.31.2.8
255.255.255.0
CUNDINAMARCA(confit)#access-list 1 permit 192.168.1.257

CUNDINAMARCA(confit)#acc
CUNDINAMARCA(confit)#interface fas

CUNDINAMARCA(confit)#interfase fastethernet 1/0
```

```
CUNDINAMARCA(confit)#acce
CUNDINAMARCA(confit)#ip access-group out
CUNDINAMARCA(confit)#
```

2.10 Los hosts de VLAN 10 en Cundinamarca si acceden a internet y no a la red interna de Tunja

```
CUNDINAMARCA(confit)#access-list 1 permit 192.168.1.257
255.255.255.0
CUNDINAMARCA(confit)#access-list 1 permit 209.17.220.0
CUNDINAMARCA(confit)#acc
CUNDINAMARCA(confit)#interface fas
CUNDINAMARCA(confit)#interfase fastethernet 0/0

CUNDINAMARCA(confit)#acce
CUNDINAMARCA(confit)#ip access-group out
CUNDINAMARCA(confit)#.
```

3 Los hosts de VLAN 30 en Tunja solo acceden a servidores web y ftp de internet.

```
TUNJA(confit)#access-list    1    permit    172.31.0.192
255.255.255.0
TUNJA(confit)#access-list 1 permit 209.17.220.0
TUNJA(confit)#acc
TUNJA(confit)#interface fas
TUNJA(confit)#interfase fastethernet 1/0
TUNJA(confit)#acce
TUNJA(confit)#ip access-group out
TUNJA(confit)#.
```

4 Los hosts de VLAN 20 en Tunja solo acceden a la VLAN 20 de Cundinamarca y VLAN 10 de Bucaramanga

```
TUNJA(confit)#access-list    1    permit    172.31.0.128
255.255.255.0
TUNJA(confit)#access-list 1 permit 172.31.1.64
TUNJA(confit)#acc
TUNJA(confit)#interface fas
TUNJA(confit)#interfase fastethernet 0/0
```

```
TUNJA(confit)#acce
TUNJA(confit)#ip access-group out
TUNJA(confit)#.
TUNJA(confit)#access-list 1 permit 172.31.2.8
TUNJA(confit)#acc
TUNJA(confit)#interface fas
TUNJA(confit)#interfase fastethernet 0/1
TUNJA(confit)#acce
TUNJA(confit)#ip access-group out
TUNJA(confit)#.
```

.

5 Los hosts de VLAN 30 de Bucaramanga acceden a internet y a cualquier equipo de VLAN 10.

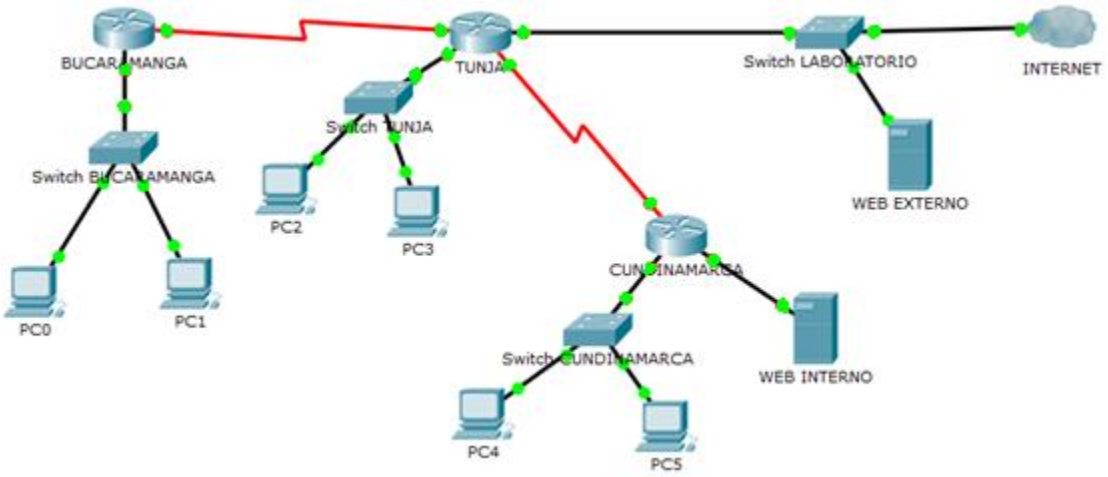
```
BUCARAMANGA(confit)#access-list 1 permit 209.17.220.0
255.255.255.0
BUCARAMANGA (confit)#access-list 1 permit any
172.31.0.0
BUCARAMANGA (confit)#acc
BUCARAMANGA (confit)#interface fas
BUCARAMANGA (confit)#interfase fastethernet 0/2
BUCARAMANGA (confit)#acce
BUCARAMANGA (confit)#ip access-group out
BUCARAMANGA (confit)#.
```

6 Los hosts de VLAN 10 en Bucaramanga acceden a la red de Cundinamarca (VLAN 20) y Tunja (VLAN 20), no internet.

```
BUCARAMANGA(confit)#access-list 1 permit 172.31.1.64
255.255.255.0
BUCARAMANGA (confit)#access-list 1 permit any
172.31.0.0
BUCARAMANGA (confit)#acc
BUCARAMANGA (confit)#interface fas
BUCARAMANGA (confit)#interfase fastethernet 0/2
BUCARAMANGA (confit)#acce
BUCARAMANGA (confit)#ip access-group out
BUCARAMANGA (confit)#.
```

```
BUCARAMANGA(confit)#access-list   1   deny   209.17.220.0
255.255.255.0
BUCARAMANGA    (confit)#access-list    1    permit    any
172.31.0.192
BUCARAMANGA (confit)#acc
BUCARAMANGA (confit)#interface fas
BUCARAMANGA (confit)#interfase fastethernet 0/2
BUCARAMANGA (confit)#acce
BUCARAMANGA (confit)#ip access-group out
BUCARAMANGA (confit)#.
```

2.11 PRUEBA DE CONECTIVIDAD:



CONCLUSIONES

El programa packet tracer permite el diseño y la configuración de los para la solución de los escenarios propuestos.

La exigencia académica del Diplomado Cisco, permitió el avance académico para el manejo de las situaciones planteadas en la problemática a abordar.

Los objetivos se cumplieron en su totalidad durante el desarrollo de la prueba de habilidades.

Existen protocolos fáciles y complejos con los cuales se puede direccionar una IP

El protocolo ayuda a que la red sea más segura y confiable, por medio de

La configuración que se necesite para salvaguardar los datos.

El protocolo EIGRP es sencillo y ayuda a saber los daños, a conocer los dispositivos vecinos, y ordenar las direcciones de las interfaces

BIBLIOGRAFIA

CICO NETWORKING ACADEMY – CCNA 1

https://static-course-assets.s3.amazonaws.com/ITN503/es/index.html

UNAD (2014). Ping y Tracer como estrategias en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

UNAD (2014). Ping y Tracer como estrategias en procesos de Networking [OVA]. Recuperado de https://1drv.ms/u/s!AmIJYei-NT1IhgTCtKY-7F5KIRC3

Cisco CCNA – configuración DHCP http://blog.capacityacademy.com/2014/01/09/cisco-ccna-como-configurar-dhcp-en- cisco-router/

CISCO. (2014). Asignación de direcciones IP. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module8/index.html#8.0.1.1

Como configurar OPSF en Router http://blog.capacityacademy.com/2014/06/23/cisco-ccna-como-configurar-ospf-en- cisco-router/

CISCO. (2014). Soluciones de Red. Fundamentos de Networking. Recuperado de https://static-course-assets.s3.amazonaws.com/ITN50ES/module11/index.html#11.0.1.1

Configuración troncal 802.1Q

https://www.cisco.com/c/es_mx/support/docs/switches/catalyst-4000-series-switches/24064-171.html